PRIVACY IMPACT ASSESSMENT
DLA HQ System Authorization Access Request (DD Form 2875)
For USE3/USE4 DLA Domains

1. **Department of Defense Component:** Defense Logistics Agency.

2. **Name of IT System:** DLA HQ System Authorization Access Requests for USE3/USE4 DLA Domains.

3. **Budget System Identification Number (SNAP-IT Initiative Number):** N/A.

4. **System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)):** N/A.

5. **IT Investment Unique Identifier (OMB Circular A-11):** N/A.

6. **Privacy Act System of Records Notice Identifier:** S500.55, entitled "Information Technology Access and Control Records."

7. **OMB Information Collection Requirement Number and Expiration Date:** N/A.

8. **Authority to collect information:** Executive Orders 10450 and 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

9. **Brief summary or overview of the IT system:** The system controls and tracks access to DLA HQ-controlled networks, computer systems, and databases for personnel assigned to DLA HQ at Fort Belvoir, Defense Energy Support Center, and Defense National Stockpile Centers. Individuals requesting access to the aforementioned provide information via a DD Form 2875, System Authorization Access Request.

10. **Identifiable Information to be Collected and Nature / Source:** PII collected from the subject individual on DD Form 2875 are individual's name, Social Security Number, citizenship, and month and date of birth.

11. **Method of information collection:** Individual provides information on DD Form 2875, entitled "System Authorization Access Request." Individuals may submit an encrypted DD Form 2875 via e-mail or a paper submission.

12. **Purpose of the collection:** The purpose of data collection is to verify an individual's identity and generate individual access account information for the DLA HQ-controlled IT networks, programs, or databases for the USE3/USE4 domains.

13. **Data uses:** Data is used to create an individual access account for DLA HQ-controlled networks, computer systems, and databases.

14. Does system derive/create new data about individuals through aggregation? No.

15. Internal and External Sharing:

Internal to DLA: The data may be shared internally as stated in the Privacy notice. All assigned personnel are to have taken Information Assurance (IA) training and thus made aware of the consequences of inappropriately using information contained therein.

External to DLA: Data may also be provided under any of the DOD "Blanket Routine Uses" published at http://www.defenselink.mil/privacy/notices/blanket-uses.html.

16. Opportunities to object to the collection or to consent to the specific uses and how consent is granted: DD Form 2875 that collects personal data contains a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data. The statement advises that participation is voluntary, and that failure to provide all the requested data may impede, delay, or prevent further processing of their request.

17. Information provided the individual at Collection, the Format, and the Means of delivery: A Privacy Act system notice was published in the Federal Register with a 30-day public comment period. Forms that collect personal data contain a Privacy Act Statement, as required by 5 U.S.C. 552a(e)(3), allowing the individual to make an informed decision about providing the data or participating in the program. Individuals may raise an objection with the DLA HQ Privacy Act Office during the comment period, during data collection, or at any time. If no objections are received, consent is presumed.

18. Data Controls:

Administrative: Users, including individuals responsible for file maintenance, receive initial and periodic refresher IA training. Users are warned through logon procedures of the conditions associated with access and the consequences of improper activities. Users are trained to lock their workstations when leaving them unattended, to log off computers when leaving at the end of the duty day. Data is periodically backed up and stored on a separate server.

Physical: DD Forms 2875 reside on a networked Exchange server initially and upon completion of the initial task, the DD Forms 2875 are manually transferred to a networked file server by IA personnel. Both servers are located in a physically-controlled building with either a badge/card swipe or read required for entry. Within buildings, servers are kept in locked or controlled access areas. Electronic records are backed up periodically. Areas housing central processing units, servers, and workstations are configured with a water-based fire suppression system. Should the system fail, the lost data could be constructed from the backup records and paper files.

Technical: The data is initially received to an Exchange mailbox and then relocated to a networked file server for storage. These systems are accredited as part of the HQ ITS Information Technology Security Certification and Accreditation process. That system uses built-in virus detection software with a notification system in place to alert all users to new viruses and software-resistant viruses. Computer terminals are password controlled or CAC-

enabled access protocols. Computer screens automatically lock upon removal of CAC PKI or after a preset period of inactivity with reentry controlled by passwording or reentering of CAC PIN.

19. Privacy Act Interface: This system is covered by a DLA Privacy Act system of records notice, S500-55, Information Technology Access and Control Records.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures:

Threats: Data is collected and used in a dedicated security mode. Data sharing occurs only among IA personnel authorized access to the mailbox or the shared network file server. Data screens are marked with the "For Official Use Only" data handling legend. All IA personnel in the Division are made aware of restrictions on secondary uses of the data records by initial and refresher IA training.

Dangers: There are no dangers in collection and storing in a networked and controlled file server. As mentioned earlier in this document, data stored is retrievable by an authorized individual within the J6FA Division.

Risks: The security risks associated with maintaining data in an electronic environment have been mitigated through administrative, technical, and physical safeguards described in this document. The safeguards in place are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the data.

21. Classification and Publication of Privacy Impact Assessment:
Classification: Unclassified.

Publication: This PIA will be published either in full or in summary form on the DLA public web site, http://www.dla.mil/public_info/efoia/privacy.asp .

DATA OWNER:
Name: [redacted] (Signature) 7/20/07 (Date)
Title: Information Assurance Officer
Work: Telephone Number [redacted]
Email: [redacted]

INFORMATION ASSURANCE MANAGER: [redacted] 7/20/2007 (Date)
Name: [redacted]
Title: Information Assurance Manager
Work: Telephone Number [redacted]
Email: [redacted]

PRIVACY TECHNOLOGY ADVISOR: [redacted] 7/25/2007 (Date)
Name: Lewis Oleinick (Signature)
Title: DLA Chief Privacy Officer
Work: Telephone Number [redacted]
Email: [redacted]

REVIEWING OFFICIAL: [redacted] 21 Aug 07 (Date)
Name: Mae De Vincentis (Signature)
Title: DLA Chief Information Officer
Work: Telephone Number [redacted]
Email: [redacted]